

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 31-03-2017			2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) 07/21/2016 to 03/31/2017	
4. TITLE AND SUBTITLE Cyberspace, the 7th Joint Function for 21st Century Warfare					5a. CONTRACT NUMBER	
					5b. GRANT NUMBER	
					5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Kenneth J. Voigt, Jr., Lt Col, USAF					5d. PROJECT NUMBER	
					5e. TASK NUMBER	
					5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)					8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton Blvd Norfolk, VA 23511-1702					10. SPONSOR/MONITOR'S ACRONYM(S)	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution is unlimited.						
13. SUPPLEMENTARY NOTES Not for Commercial Use without the express written permission of the author.						
14. ABSTRACT Today's military leaders face a challenge in understanding how warfare has changed with the advent of the cyberspace domain. The cyberspace domain is best viewed as an enabling domain on the information age battlefield for military planners to effectively utilize in combat. However, recognition that cyberspace is a domain and that it is an integral part of warfare means nothing unless it can be incorporated into the operational level of war and employed within the operational art. The speed of cyberspace, coupled with the seemingly unlimited distance of the domain, are different than the natural domains and require require cyberspace to be looked at as a joint function to integrate, synchronize, and direct operations.						
15. SUBJECT TERMS Cyberspace, operational art, operational design, joint functions						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			Director of JAWS	
Unclassified	Unclassified	UNCLASS	Unclassified Unlimited	55	19b. TELEPHONE NUMBER (Include area code) 757-443-6301	

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL



**CYBERSPACE; THE 7TH JOINT FUNCTION FOR 21ST CENTURY
WARFARE**

by

Kenneth J. Voigt, Jr.

Lieutenant Colonel, United States Air Force

CYBERSPACE, THE 7TH JOINT FUNCTION FOR 21ST CENTURY WARFARE

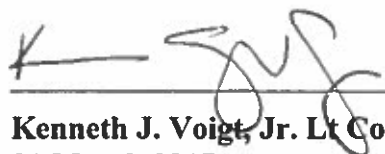
by

Kenneth J. Voigt, Jr.

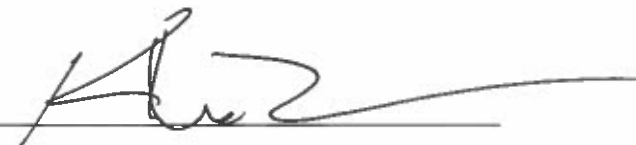
Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.


Signature: 
Kenneth J. Voigt, Jr. Lt Col, USAF
31 March 2017

Thesis Advisor:

Signature: 
Keith Dickson, Ph.D.
Professor of Military Studies, JAWS
Thesis Advisor

Approved by:

Signature: 
Kevin Therrien, Col, USAF
Committee Member

Signature: 
Stephen Rogers, COL, USA
Director, Joint Advanced Warfighting School

ABSTRACT

Today's military leaders face a challenge in understanding how warfare has changed with the advent of a man-made cyberspace domain. The cyberspace domain is best viewed as an enabling domain on the information age battlefield for military planners to utilize effectively in combat. However, the recognition that cyberspace is a domain and that it is an integral part of warfare means nothing unless it can be incorporated into the operational level of war and employed within the operational art. Unfortunately, there is limited literature focused on how a joint force commander (JFC) will utilize cyberspace.

The speed of cyberspace, coupled with the seemingly unlimited distance of the domain, are different than the natural domains and require cyberspace to be looked at as a joint function to integrate, synchronize, and direct operations for a JFC. The information age battlefield requires the integration of cyberspace capabilities at the operational level.

Cyberspace added as the seventh joint function would define how a JFC can properly integrate cyberspace into a given campaign's operational design. A cyberspace function would enhance, support, and enable the other joint functions to provide a JFC the ability to create a 21st-century operational design. Each combatant commander must effectively integrate the cyberspace domain to enable fires, intelligence, C2 and protection for 21st-century warfare. Viewing cyber as the seventh function would ensure that a JFC can integrate cyberspace across the campaign's operation design.

DEDICATION

To my wife and children, whose patience and understanding were instrumental in completing this thesis.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION.....	1
CHAPTER 2: CURRENT CONSIDERATIONS on OPERATIONAL USE	
THE INFORMATION AGE BATTLEFIELD.....	6
CYBERSPACE AS A WEAPON.....	7
CYBERSPACE AS A COMPONENT.....	10
CYBER MISSION FORCE.....	12
INTEGRATION REQUIREMENT.....	16
CHAPTER 3: CYBERSPACE OPERATIONAL DESIGN.....	19
ROLE OF JOINT FUNCTIONS.....	20
CYBERSPACE AND OPERATIONAL DESIGN.....	22
RUSSIA-GEORGIA WAR CASE STUDY.....	27
CHAPTER 4: RECOMMENDATIONS.....	34
CHAPTER 5: CONCLUSION.....	37
BIBLIOGRAPHY.....	40
VITA.....	47

CHAPTER 1: INTRODUCTION

“The U.S. military is no more capable of operating without the Internet than Amazon.com would be.” — Richard A. Clarke, *Cyberwar*¹

In the aftermath of World War I, military leaders and theorists sought to understand what had caused warfare to change so significantly. With the disastrous losses of the Great War's defensive stalemate still in their minds, some theorists, like Giulio Douhet and William Mitchell, concentrated on how technological advances in air warfare would be the deciding factor in future wars.² However, it was the Soviet theorist, Georgii S. Isserson who looked at the lessons of World War I as a revolutionary change to warfare that removed the commander's ability to see enemy formations and positions. Isserson argued that the employment of artillery, tanks, and aircraft required the commander to think about a campaign differently and apply operational art.³ Isserson defined operational art as a necessary link for multiple separate tactical actions “linked in depth, and united by the general intent.”⁴ According to Isserson, the main reason for the strategic stalemate of the First World War was the inability to use operational art to tie tactical actions together to meet operational objectives.⁵ Isserson's analysis can help

¹ Richard A. Clarke and Robert K. Kane, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: Ecco, 2010), 93.

² Giulio Douhet and Brigadier General William “Billy” Mitchell were the outspoken proponents of the benefits of airpower. Douhet's theory of victory in combat through massive aerial bombardment can be explored further in his book, *The Command of the Air*. Translated by Dino Ferrari. (Washington, DC: Office of the Air Force History, 1983). Mitchell's views on the primacy of airpower can be further studied in his book, *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military*, 2d ed., (Tuscaloosa, AL: University of Alabama Press), 2010.

³ Georgii Samoilovich Isserson, *The Evolution of Operational Art*, translated by Bruce W. Menning, (Fort Leavenworth, KS: Combat Studies Institute Press, 2013), 16-17.

⁴ Ibid.

⁵ Ibid, 26, 35.

frame an understanding of the next evolution in warfare, 21st-century battlefield which includes a new domain of cyberspace.

Today's military leaders face a similar challenge in understanding how warfare has changed with the advent of a man-made cyberspace domain.⁶ Some argue, as Douhet and Mitchell did, that cyberspace should be treated as a new domain equal to the air, land, space, and maritime domains. Others claim that it is a unique entity, a key to warfighting that alone will win our nation's wars.⁷

The man-made domain is less a panacea and more like an enabling domain on the information age battlefield for military planners to utilize cyberspace effectively in combat. Isserson defined the modern battlefield regarding of a recognition of a change in space and time.⁸ Cyberspace has only extended this space-time construct further. In the information age, military forces are dependent on cyberspace for effective weapons employment, command and control of forces, positioning and resupplying of forces, and conduct of intelligence operations.⁹ The Chairman of the Joint Chiefs of Staff recognizes cyberspace as an "integral part of armed combat," required by the joint force to meet operational and strategic objectives.¹⁰

⁶ There are many different definitions of cyberspace throughout current literature. This paper uses the U.S. Joint Chiefs of Staff definition of cyberspace, a "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems and embedded processors and controllers." U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*. (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 (As Amended Through February 15, 2016)), 58.

⁷ Clarke and Kane, *Cyber War*, 31.

⁸ Isserson, *Operational Art*, 16-26.

⁹ Clarke, 227.

¹⁰ U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, (Washington, DC: U.S. Joint Chiefs of Staff, September 10, 2012), 2.

To meet the Joint Chief's vision for globally integrated operations, a cyberspace discussion must reflect Isserson's operational art analysis and address how a joint force commander (JFC) will incorporate cyberspace to enable joint operations to meet the timing and tempo demands of the 21st-century battlefield.¹¹ Unfortunately, there is a dearth of literature focused on how a JFC will utilize cyberspace. Cyberspace advocates believe that cyberspace is a uniquely new and separate domain and have focused on command and control, addressing only authority and permission issues, reflecting the assumption that authority to use force within cyberspace is unique to the cyberspace domain. Instead of concentrating on the command and control (C2) structure, others believe that cyberspace is a unique entity that changes the nature of warfare and have advocated for an operational cyberspace framework to shape operational art and operational design to support a JFC's planning and execution.¹²

Information age domain integration is much more than a discussion of who, but rather more about how JFCs can utilize cyberspace at the operational level of war.¹³ Recognition of cyberspace as a function derives from how integral the 21st-century domain is in enabling the JFC's operational design. The changes in information age space and time, combined with cyberspace dependency, requires an operational design that

¹¹ U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, 5.

¹² William S. Angerman, *Cyber Power for the Joint Force Commander: An Operational Design Framework*, Master's Thesis, (Norfolk, VA: Joint Advanced Warfighting School, 2014), 11.

¹³ U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, JP 1 defines the operational level as one which, "links strategy and tactics by establishing operational objectives needed to achieve the military end states and strategic objectives. It sequences tactical actions to achieve objectives. The focus at this level is in the planning and execution of operations using operational art: the cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means. JFCs and component commanders use operational art to determine when, where, and for what purpose major forces will be employed and to influence the adversary's disposition before combat. Operational art governs the deployment of those forces and the arrangement of battles and major operations to achieve operational and strategic objectives" I-8.

integrates cyberspace for synchronized joint operations. The speed of cyberspace, coupled with the seemingly unlimited distance of the domain, are different than the natural domains and require a look at cyberspace as a joint function to integrate, synchronize, and direct operations for a JFC. Cyberspace capabilities that enable a JFC to integrate, synchronize, and direct joint operations to integrate cyberspace into a given campaign's operational design. Cyberspace as a joint function reverses barriers to integration and demonstrates an understanding of cyberspace as a glue binding and enabling all other joint functions. This paper recommends adding cyberspace as a joint function to enhance a JFC's application of operational art in the 21st century.

Research Approach

Doctrine is the best primer to establish how a JFC can integrate the cyberspace domain. *JP 3-0, Joint Operations*; *JP 3-60, Joint Targeting* and *JP 5-0, Joint Operation Planning* define current joint functions, the joint targeting cycle, operational design, and operational art. These concepts demonstrate the need to view cyberspace as a new joint function to enable 21st-century operational art. Current joint doctrine could be modified to include cyberspace as a new function. An overview of how military theorists transformed warfare after the First World War illustrates the emergence of operational art. The theorists recognized what had changed and evaluated how these changes had influenced the conduct of warfare, and how those changes should be incorporated into doctrinal precepts to guide future operational art. The method these theorists used to integrate 20th-century technology to maneuver warfare will serve as a model to for how operational art in the 21st-century must employ cyberspace within an operational design.

Cyberspace as a joint function can better prepare operational level planners to integrate targeting, intelligence preparation of the battlefield, and overall operational design.

The 2008 Russia-Georgia War will be presented as a case study to illustrate cyberspace as an enabling function for other joint functions. It is apparent the Russians have already deciphered the basics of integrating cyberspace as a joint function at the operational level. Combining the concepts of operational cyberspace integration with historical analysis should demonstrate that the 21st-century battlefield requires a fully integrated cyberspace capability into operational design as a joint function.

Isserson recognized the need for an operational level of war to integrate new capabilities in such a way that would allow a commander to dominate the battlefield. In the same way, the information age battlefield requires the integration of cyberspace capabilities at the operational level. Joint force commanders must effectively integrate and synchronize cyberspace to enable fires, intelligence, C2, and protection to dominate the 21st-century battlefields.

CHAPTER 2: CURRENT CONSIDERATIONS on OPERATIONAL USE

"It was senseless to break down the door if there was no one to go through it."
— Georgii S. Isserson, *The Evolution of Operational Art*¹

THE INFORMATION AGE BATTLEFIELD

The 21st-century battlefield bears only superficial similarities to the 20th-century battlefield. There is a fundamental difference to the way wars are fought and will be fought in the information age due to the speed and depth of cyberspace. The advancements in information technology may very well limit traditional 20th-century maneuver warfare fought in the domains of air, land, and sea.² The 2014 Quadrennial Defense Review has recognized the ongoing change, describing an “increasingly contested battlespace in the air, sea, and space domains.”³ In recognition of the significance of cyberspace to modern warfighting, the Department of Defense (DoD) has defined cyberspace as a separate domain and highlighted its importance to achieving the national interests.⁴ The Joint Staff has declared that warfare in the information age will be defined by the reliance on integrated and synchronized cyberspace operations.⁵

¹ Isserson, *Operational Art*, 37.

² Jeffrey M. Reilly, “Multidomain Operations: A Subtle but Significant Transition in Military Thought,” *Air and Space Power Journal* 30, Issue 1 (Spring 2016): 61.

³ U.S. Department of Defense, *Quadrennial Defense Review*, (Washington DC: U.S. Department of Defense, 2014), III.

⁴ *Department of Defense Strategy for Operating in Cyberspace*, (Washington, DC: U.S. Department of Defense), July 2011, 5. The DoD defines the cyberspace domain as a, “global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,” U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, (Washington, DC: U.S Joint Chiefs of Staff, November 8, 2010 (As Amended Through February 15, 2016)), 58

⁵ U.S. Joint Chiefs of Staff, *Capstone Concept*, 2.

Recognition that cyberspace is a domain and that it is an integral part of warfare means nothing unless it can be incorporated into the operational level of war and employed within the commander's operational art. Joint planners need to understand how this information revolution equates to a change in warfare at the operational level, and how JFCs can plan operations on the 21st-century battlefield. Just as the advent of mechanization, wireless communication, and aircraft changed warfare at the operational level in the decades after 1918, so too has cyberspace changed warfare in the 21st-century. This shift in warfare requires a proper conceptualization of cyberspace.

This chapter will examine this conceptualization. By examining the debate over cyberspace domain's use to deliver unique weapons, the chapter will look at current C2 constructs for cyberspace, which argues that the man-made domain must be centrally managed. In contrast, historical examples will be presented to discount the view that new technology is a warfighting panacea. Such an approach rarely achieves operational or strategic objectives. A proper conceptualization of 21st-century warfare and the role of cyberspace will yield an understanding that cyberspace is better integrated into joint operations as a joint function.

CYBERSPACE AS A WEAPON

In the spirit of airpower advocates in the early 20th-century, cyberspace enthusiasts are quick to paint a picture of cyberspace operations quickly crippling a country. Richard Clarke, the special advisor to the president for cyberspace for both President Bill Clinton and President George W. Bush, envisioned cyberspace weapons bringing down over 150 U.S. cities in less than fifteen minutes, crippling infrastructure

and preventing a military response.⁶ The speed and power of the cyberspace domain seem to be almost unimaginable. The theory is that since many societies have become reliant on cyberspace for communications, trade, and comfort, it follows that cyberspace attacks could jeopardize patterns of life more effectively than aerial bombing or artillery barrages.⁷

In the view of Clarke and others, cyberspace has become the delivery platform for the next great weapon, one that can deter adversaries, and if needed, can be the sole weapon to achieve national objectives.⁸ In 1921, Giulio Douhet surmised a similar theory on the destructive capability of airpower. Douhet believed that airpower had the ability to inflict “grave damage as to bring about a complete collapse of his forces in a very few days.”⁹ Airpower enthusiasts thought offensive aircraft alone could quickly and decisively force an adversary to capitulate. To enthusiast like Douhet, the aircraft alone would dominate the battlefield. William Mitchel expounded on Douhet’s theory by proclaiming that surface navies and land forces were no longer required since airpower could defend against enemy air and ships as well as project power on vital land targets.¹⁰

History has shown that Douhet and Mitchell were mistaken. Airpower alone could not decisively meet a nation's desired end state in war. Instead, air, land, and sea forces synchronized and integrated at the operational level became the winning formula for 20th-century maneuver warfare. Likewise, the integration and synchronization of

⁶ Clarke and Kane, *Cyber War*, 67.

⁷ Elizabeth A. Myers, *Cyber as a “Team Sport”: Operationalizing a Whole-of-Government Approach to Cyberspace Operations*, Master’s Thesis, (Norfolk, VA: Joint Advanced Warfighting School, 2011), 17.

⁸ Corey M. Ramsby and Panayotis A. Yannakogeorgos, “A Reality Check on a Cyber Force.” *Strategic Studies Quarterly* 10, no. 2: 116-133. *International Security & Counter Terrorism Reference Center*, EBSCOhost (accessed September 1, 2016): 119.

⁹ Douhet, *The Command of the Air*, 51.

¹⁰ Mitchell, *Winged Defense*, 109.

cyberspace with air, land, and sea weapons will demonstrate the real potential of information age warfare. Analogous to airpower, cyberspace power should be understood as another capability that a JFC can use in combination with other capabilities to achieve a decisive result.¹¹ Just as airpower's actual effectiveness was demonstrated as an integrated capability, history indicates the same role for cyberspace.

The faith cyberspace advocates have in a single capability is reminiscent of the reliance on the tank as the only answer to the stalemate on the Western Front between 1916 and 1918. German Major-General Heinz Guderian discovered in his analysis of armored tactics in World War I that the Allies' overconfidence in their new weapon - the tank - caused them to squander its tactical and strategic advantage. The first uses of the tank in 1916 proved indecisive.¹²

The Allies, through trial and error, developed a combined arms approach one year later at Cambrai that synchronized the movement of the infantry, cavalry, aircraft, and artillery to integrate fire, maneuver, and protection.¹³ The battle of Cambrai provided the British and French commanders operational success on the battlefield not seen in the three previous years of the Great War. Guderian used the lessons from this battlefield and others that followed to develop a modern concept of maneuver warfare that opened a new chapter in the history of warfare.¹⁴

Cyberspace advocates who view cyberspace as a separate and decisive capability are the modern counterparts of those in 1916, who believed the tank was the answer to

¹¹ Peter W. Singer, "The War of Zeros and Ones," *Popular Science*, (2014): 43, 46.

¹² Heinz Guderian, *Achtung-Panzer!*. Translated by Christopher Duffy, (London: Brockhampton Press, 1999), 72.

¹³ Ibid 79-85.

¹⁴ Ibid, 7.

changing the battlefield decisively. Likewise, Duohet's and Mitchell's inaccurate assessment of airpower as the only necessary instrument for decisive action on the battlefield should cause cyberspace advocates to pause.

The categorization of cyberspace as a sole decisive weapon not only discounts 20th-century lessons related to the evolution of warfare, but it also limits cyberspace to a simple concept, reducing this capability to what some have described as a "one-and-done" weapon.¹⁵ History demonstrates that the best path to operational and strategic success is to integrate and synchronize capabilities at the operational level. There are cyberspace advocates who understand the need to integrate, but they believe cyberspace control and direction must be removed from the operational commander and placed only in the hands of suitable experts who can employ this capability effectively at the request of the commander.

CYBERSPACE AS A COMPONENT

Cyberspace theorists believe that the uniqueness of cyberspace requires a unique C2 model. U.S. Cyber Command (USCYBERCOM) advocates its role to act as the supported or supporting command to integrate cyberspace into the "broader range of military operations."¹⁶ Because this point of view reflects the idea that cyberspace is equivalent to the terrestrial domains, proponents argue that the best way to integrate cyberspace is to organize cyberspace forces like how terrestrial domains are organized by a component model. The belief is a cyberspace component would provide a JFC with

¹⁵ Richard J. Bailey, Jr., "Dilating Pupils: The Pedagogy of Cyber Power and the Encouragement of Strategic Thought," *Air and Space Power Journal Africa & Francophonie*, 7, Issue 3 (Fall 2016): 18.

¹⁶ U.S. Cyber Command, *Beyond the Build, Delivering Outcomes through Cyberspace: The Commander's Vision and Guidance for U.S. Cyber Command*, (Fort Meade, MD: Department of Defense, June 3), 2015, 7.

consolidated expertise which will result in “integrated cyberspace operation(s).”¹⁷ Others have advocated that the owning command, USCYBERCOM, can direct the assignment and apportionment of cyberspace forces and temporarily assign tactical control to theater commanders for a particular mission.¹⁸

USCYBERCOM centralized control of cyberspace by standing up Joint Forces Headquarters-Cyber (JFHQ-C) in a direct support role. JFHQ-C provides USCYBERCOM the ability to maintain authorities over cyberspace forces and rely on a coordination element dispatched to each combatant commander to synchronize cyberspace actions.¹⁹ In theory, this model affords USCYBERCOM the ability to support combatant commanders while simultaneously supporting more strategic missions operationally.²⁰ This structure reflects USCYBERCOM’s desire to centralize and control cyberspace authorities. Centralized control from USCYBERCOM enables cyberspace forces and capabilities to function as a separate domain, but not integrated or synchronized with JFC operations. At best this close control model affords cyberspace forces the ability perform scripted or coordinated operations with JFCs.

The C2 models of the last century were based on the ability to coordinate actions across domains. Cyberspace operations, either offensive or defensive, occur at speeds faster than traditional C2 models can coordinate with other elements of military power. The current cyberspace philosophy that cyberspace must be centrally controlled as a

¹⁷ Ben FitzGerald and Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control*, Disruptive Defense Papers, (Washington, DC: Center for a New American Security, April, 2014), 9-10; Brett T. Williams, “Ten Propositions Regarding Cyberspace Operations,” *JFQ: Joint Force Quarterly* no. 61 (2011 2nd Quarter 2011): 11; and Sean C.G. Kern, “Expanding Combat Power Through Military Cyber Power Theory,” *Joint Forces Quarterly* 79 (4th quarter 2015), 89.

¹⁸ FitzGerald and Wright, *Digital Theaters*, 9.

¹⁹ *Ibid.*, 8.

²⁰ *Ibid.*

capability package delivered to the commander violates the doctrinal principles of unity of command and simplicity for joint operations.²¹ USCYBERCOM and advocates for centrally controlled cyberspace have fallen into a similar mindset as the airpower advocates in the interwar period. Air commanders refused to integrate forces functioning separately and offered limited support to other commanders with strict limitations on employment and command authorities. The result during wartime was a lack of understanding between air and ground forces for integrating capabilities, the product of a bifurcated C2 structure, which proved ineffective in the initial 1942 U.S. campaign in North Africa.²² The lessons of 1942's ineffective and limited C2 structures can be applied today to the requirement of integrated and synchronized cyberspace on a 21st-century battlefield. USCYBERCOM appears to recognize the limitation of centrally controlling cyberspace that is geographically separated from the operational environment. In an attempt to streamline cyberspace operations, USCYBERCOM adapted to a new C2 model, a Cyber Mission Force.

CYBER MISSION FORCE

²¹ U.S. Chairman of the Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0. (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), A-1 – A-5 establishes 12 principles of joint operations: objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, simplicity, restraint, perseverance, and legitimacy. JP 3.0 states, "The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective. Unity of command means that all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose." Simplicity is defined as a principle, "to increase the probability that plans and operations will be executed as intended by preparing clear, uncomplicated plans and concise orders."

²² F. Randall Starbuck outlines the challenges of the different C2 architectures for U.S. airpower during Operation Torch in his thesis, *Airpower in North Africa, 1942- 43: An Additional Perspective*, (Carlisle Barracks, PA: U.S. Army War College, 1992). His thesis is not an in-depth historical analysis of Operation Torch, but more of a look at the training and command and control structure for the operation. Throughout the thesis, Starbuck points out the limitations of coordination between distant commanders, lack of understanding between ground and air forces due to separate chains of command and lack of training and gaps in doctrine that was formulated off the Douhet concept of strategic bombing. Starbuck illustrated how the theater commander eventually changed the C2 model to better integrate airpower with the operational plan, thus removing the ground force notion of "umbrella" air defense and strategic bombing mission out of sync with operational timing and tempo, 13-14, 32-33.

The DoD has invested manpower, time, and funds to create the Cyber Mission Force as the cornerstone of cyberspace C2 and force structure to support a JFC.²³ The Cyber Mission Force is separated into three parts: Cyber Protection Teams, Combat Mission Teams, and National Mission Forces.²⁴ The Combat Mission Team and Cyber Protection Team are the parts of the Cyber Mission Force which are designed to support operational level commanders. Cyber Protection Teams are organized to, “defend priority DoD networks and systems against priority threats.”²⁵ Operational level offensive cyberspace support is provided via the Combat Mission Team.²⁶

USCYBERCOM views the Cyber Mission Force as a capability able to provide “full-time, global” cyberspace support to JFCs.²⁷ The Cyber Mission Force follows the direct support model controlled by the respective lead service JFHQ-C.²⁸ Admiral Michael Rogers, commander USCYBERCOM, considers the direct support model as essential for providing operational level commanders the expertise and tools required to execute their respective mission in the cyberspace domain.²⁹ Direct support provides centrally planned and executed cyberspace missions in close coordination with a JFC. The Cyber Mission Force also bifurcates offensive and defensive cyberspace operations

²³ U.S. Department of Defense, *Quadrennial Defense Review*, 33.

²⁴ Ibid. Earlier publications, such as U.S. Department of Defense. *Mission Analysis for Cyber Operations of Department of Defense*. (Washington, DC: U.S. Department of Defense, August 2014) and the U.S. Congress Senate Armed Services Committee, *Statement of Admiral Michael S. Rogers, USN, Commander, United States Cyber Command*. 114th Cong., 2nd sess., April 5, 2016, describe this force as a “Combat Mission Team.” The 2014 QDR and 2015 DoD Cyber Strategy both title the force as a “Combat Mission Force.” For means of continuity, this paper will utilize the title “Combat Mission Team.”

²⁵ *Department of Defense Strategy for Operating in Cyberspace*, 6.

²⁶ U.S. Department of Defense. *Mission Analysis for Cyber Operations of Department of Defense*. (Washington, DC: U.S. Department of Defense, August 2014), 9.

²⁷ U.S. Congress. Senate, Armed Services Committee. *Statement of Admiral Michael S. Rogers, USN, Commander, United States Cyber Command*, 7.

²⁸ U.S. Department of Defense. *Mission Analysis for Cyber Operations of Department of Defense*, 10.

²⁹ “An Interview with Michael S. Rogers.” *Joint Force Quarterly* no. 80 (2016 1st Quarter 2016): 82.

by separating the roles on different static teams: Cyber Protection Teams for defense and Cyber Mission Teams for offense.

When writing about the maritime domain about a century ago, Sir Julian Corbett argued that offensive and defensive operations are mutually complementary and that wars are not solely offensive or defensive.³⁰ Corbett's argument can also be applied to the global commons of cyberspace. As Corbett pointed out, "there is never, in fact, a clean choice between attack and defense. In aggressive operations the question always is, how far must defense enter into the methods we employ to enable us to do the utmost within our resources to break or paralyse the strength of the enemy."³¹ Like the maritime domain, cyberspace domain operations require an ability to plan, synchronize, and quickly transfer between offensive and defensive missions.³² This clearly cannot be done under the Cyber Mission Force construct.

Corbett's analysis of offensive and defensive operations in the maritime domain led to his dissection of an ability to command the sea. A state could not conquer the sea, but rather needed to look at what the state needed to "secure for ourselves, and what it is we can deny the enemy."³³ To Corbett, the importance of the sea was the ability to control access to maritime lines of communications, and thus lead to a strategy to deny the enemy those lines of communication, while enabling the state to exploit its access.³⁴ Corbett viewed the sea domain as a global common, whose "offence and defence tend to merge in a way unknown ashore."³⁵

³⁰ Julian S. Corbett, *Some Principles of Maritime Strategy*, (New York: Dover Publications, 2004), 13.

³¹ *Ibid*, 14.

³² Ryan Tate, "Maximizing Flexibility: Mitigating Institutionalized Risk in the Cyber Mission Force." *The Cyber Defense Review* (June, 2016): 1.

³³ Corbett, *Some Principles of Maritime Strategy*, 56.

³⁴ *Ibid*.

³⁵ *Ibid*, 62.

Cyberspace is analogous to the global sea domain, thus requiring that a JFC the ability to act offensively and defensively in cyberspace simultaneously, and plan synchronized operations across all domains. The main difference between the maritime domain and the cyberspace domain is speed. Centralized control and distribution are no more useful for naval forces than for cyberspace capabilities. As a force distributed to a JFC, the Cyber Mission Force will have a difficult time coordinating operations across two separate teams when operations occur at the speed of light. As Corbett pointed out with the maritime domain, “the paramount concern . . . is to determine the mutual relations of your army and navy in a plan of war.”³⁶ Again, cyberspace requires the same approach Corbett took with the sea and focus on the relationship to employ cyberspace capabilities across the operational plan.

Further complicating the Cyber Mission Force effectiveness, is the divided planning structure. Joint Publication 3-12 (R), *Cyberspace Operations*, recognizes that the reliance a JFC has on cyberspace requires that operational level leaders need to “fully integrate [cyberspace operations] into joint operation planning and execution . . .” processes.³⁷ However, the current direct support model of centralized cyberspace planning in coordination with a JFC makes integrated planning a difficult endeavor. Well-intentioned planners, separated by the offensive or defensive skillsets and under a different operational command chain tend to miss the relationship between effects and objectives.³⁸ Joint Publication 3-60, *Joint Targeting*, highlights the requirement for a JFC

³⁶ Ibid, 2.

³⁷ U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R). (Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013), I-6.

³⁸ Jason M. Bender, “The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations,” *Small Wars Journal* 9, no. 11 (November 2013), 2.

to tie objectives to the national end state. It is from these objectives that effects, targets, and targeting platforms are derived.³⁹ The design a centrally controlled Cyber Mission Force in direct support of operational level commanders is grounded in the belief that cyberspace impacts all regions simultaneously. Unfortunately, the Cyber Mission Force C2 construct inhibits a JFC's flexibility and ability to utilize cyberspace fully.

JFCs require an ability to build a plan for freedom of maneuver across all domains, to include cyberspace, through integrated and synchronized capabilities to meet the desired effect on all targets regardless of the weapon system. However, in the Department of Defense report, "Mission Analysis for Cyber Operations of the Department of Defense," the department argues that the Cyber Mission Force direct support model should only be a temporary command and control structure until the domain matures.⁴⁰

INTEGRATION REQUIREMENT

A former USCYBERCOM J3, Major General Brett Williams, observed there is an inherent need to integrate cyberspace operations to avoid limiting a JFC's flexibility.⁴¹ Other cyberspace advocates believe that the uniqueness of cyberspace requires separate C2 structures and separate authorities to support operational level commanders who can utilize a synchronized and integrated cyberspace domain.⁴² However, according to JP 3-12 (R), "the pace of [cyberspace operations] requires significant pre-operational collaboration, as well as constant vigilance upon initiation, to ensure that activities in

³⁹ U.S. Joint Chiefs of Staff, *Joint Targeting*, Joint Publication 3-60. (Washington, DC: Joint Chiefs of Staff, January 31, 2013), I-2.

⁴⁰ U.S. Department of Defense. *Mission Analysis for Cyber Operations of Department of Defense*. Washington, 25.

⁴¹ Williams, "Ten Propositions Regarding Cyberspace Operations," 15.

⁴² Brett Reister, *Cyberspace: Regional and Global Perspectives*, Strategic Research Project, (Carlisle Barracks, PA: U.S. Army War College), 2012, 1.

cyberspace and throughout the [operational environment] are coordinated and deconflicted in advance."⁴³ Cyberspace operations planning is likened to how operational level planners execute fire coordination for the "rapid engagement of targets and simultaneously provides safeguards for friendly forces."⁴⁴

A JFC's ability to synchronize cyberspace operations with the other terrestrial based domains is the key to effective cyberspace domain operations. The comparison to fire support planning is useful, as the same analogy can be made for synchronizing cyberspace efforts with a JFC's intelligence, C2, movement and maneuver, and protection efforts. JP 3-0 states, "joint functions reinforce and complement one another, and integration across the functions is essential to mission accomplishment," and that, "the JFC can choose from a wide variety of joint and Service capabilities and combine them in various ways to perform joint functions and accomplish the mission."⁴⁵ As joint doctrine indicates, because cyberspace capabilities span across all joint operations, a JFC requires an ability to synchronize with all operational planning and execution processes.

The information age battlefield presents a JFC with a different view of domain employment, one of interdependence versus integration.⁴⁶ Dr. Jeffrey Reilly defined domain interdependence as one where "failure in one domain has cascading effects in one or more of the others."⁴⁷ It is this domain interdependence that other nations are learning to exploit and are developing methods to integrate the domains successfully while

⁴³ U.S. Joint Chiefs of Staff, *Cyberspace Operations*, IV-9.

⁴⁴ Ibid.

⁴⁵ U.S. Joint Chiefs of Staff, *Joint Operations*, III-1.

⁴⁶ Jeffrey M. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," *Air and Space Power Journal* 30, Issue 1 (Spring 2016): 67.

⁴⁷ Ibid.

denying that opportunity to others.⁴⁸ All modern military forces depend on the ability to integrate technology into operations; this is especially true for a JFC.⁴⁹ The understanding that 21st-century warfare requires interdependence over integration necessitates a decentralized operational level command and authorities structure for cyberspace.

The complexity of 21st-century battlefields requires that a JFC plans, synchronizes, and integrates cyberspace throughout the operational design. Cyberspace is a unique domain; it is an enabling domain for 21st-century warfare. As an enabling domain, one can look at the cyberspace as both a domain and a function to integrate, synchronize, and enable the other six functions on the information age battlefield. Warfare in the information age requires a shift from trying to integrate cyberspace operations into a theater to understanding that cyberspace operations are instrumental for theater operations. Close coordination and integration are the lethargic 20th-century techniques, full synchronization of operations is the prerequisite for this century's warfare. According to Joint Publication 3.0, *Joint Operations*, "related capabilities and activities grouped together to help the JFC integrate, synchronize and direct joint operations" are joint functions.⁵⁰ Each joint force commander must effectively integrate the cyberspace domain to enable fires, intelligence, C2, and protection for 21st-century warfare. Viewing cyberspace as the seventh function ensures that a JFC can integrate cyberspace across the campaign's operation design.

⁴⁸ U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035*, (Washington, DC: Joint Chiefs of Staff, July 14, 2016), 15.

⁴⁹ Ibid, 16.

⁵⁰ U.S. Joint Chiefs of Staff, *Joint Operations*, III-1.

CHAPTER 3: CYBERSPACE OPERATIONAL DESIGN

"I have every confidence in the ultimate success of our joint cause; but success in modern war requires something more than courage and a willingness to die: it requires careful preparation." — General Douglas MacArthur¹

Operational design is rooted in a commander's ability to understand and apply operational art. Isserson saw the value of operational art as an ability to move from a series of tactical battles to continuous combat operations throughout the depth of the battlefield.² U.S. experiences on the 20th-century battlefield have developed a doctrine which reflects Isserson's value of operational art. U.S. doctrine defines operational art as, "the application of creative imagination by commanders and staffs—supported by their skill, knowledge, and experience," that is used to "link ends, ways, and means to achieve the desired end state."³ Operational art is described in doctrine as a "thought process" which, "promotes unified action," by synchronizing tactical actions to the overall end state and "thereby promoting unity of effort."⁴ Similar to Isserson's analysis, JP 3-0, *Joint Operations*, states that "without operational art, campaigns and operations would be sets of disconnected events."⁵ Understanding how distinct capabilities can integrate and synchronize for unity of effort is "essential to meet the complex challenges facing the U.S."⁶

¹ Edward T. Imparatov, *General MacArthur Speeches and Reports 1908-1964*, (Paducah, KY: Turner Publishing Company, 2000), 124.

² Isserson, *Operational Art*, 48

³ U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0, (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), III-1.

⁴ U.S. Joint Chiefs of Staff, *Joint Operations*, II-3.

⁵ *Ibid*, II-4.

⁶ U.S. Joint Chiefs of Staff, *Joint Operation Planning*, III-4.

Joint functions provide a JFC with combined capabilities which “help the JFC integrate, synchronize, and direct joint operations” for operational unity of effort.⁷ Joint functions are a collection of joint and Service capabilities that combine to meet mission objectives.⁸ This chapter will examine the inclusion of cyberspace as a joint function to synchronize operations and adjust operational art and operational design for the 21st-century battlefield.

ROLE OF JOINT FUNCTIONS

There are six joint functions in current U.S. doctrine: C2, intelligence, fires, movement and maneuver, protection, and sustainment. All of these functions are a grouping of joint capabilities that provide a JFC an ability to combine joint and coalition capabilities in a synergistic effect to meet the operational and strategic objectives. JP 3-0, *Joint Operations*, states that “joint functions reinforce and complement one another, and integration across the functions is essential to mission accomplishment.”⁹ The traditional 20th-century joint functions are not organized by component, domain, or specific forces. Instead, a JFC applies experience and expertise to combine disparate capabilities together in a carefully planned and orchestrated operation.

Joint functions assist a JFC in integrating and synchronizing individual service, component, and domain capabilities throughout the area of operations to dominate the battlefield. A joint functions approach allows a JFC to build a plan based on meeting

⁷ U.S. Joint Chiefs of Staff, *Joint Operations*, III-1.

⁸ Ibid.

⁹ Ibid.

operational objectives by combining the best service, domain, or component capability within the operational design.¹⁰

The current cyberspace employment concept is organized more for strategic employment and creates barriers to operational integration, which can limit the operational design of JFC's use of cyberspace.¹¹ Major General Brett Williams, former USCYBERCOM J3, noted that, "global control does not provide the integration, responsiveness and agility necessary for cyberspace operations at the theater level."¹²

At the turn on the 20th-century, Isserson analyzed the change in warfare with the advent of maneuver operations. He concluded that there was a need to connect strategic objectives with operational art to connect individual tactical action in depth and breadth. The change in timing and tempo of 21st-century warfare necessitates a change in the operational art to enable a commander to plan and execute at the speed of cyberspace - the speed of light. A cyberspace function allows a commander to create an operational design which meets the speed of an information age battlefield.

To seize the initiative and shape the battlefield, operational level leaders require agility and speed of maneuver in cyberspace that must be embedded throughout the plan. This means separating cyberspace from preconceived peacetime C2 structures and coordination practices to a function that is integrated and synchronized throughout the operational design. Separating cyberspace planning from the JFC limits the effectiveness of the new domain as, "actionable knowledge of this domain at the operational level will

¹⁰ Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations." (*Joint Forces Quarterly* 73 (2nd quarter 2014)), 14, Both Williams and Angerman, 37 have argued that cyberspace looks like the other joint functions, representing both the noun (capability) and the verb (activity). See Angerman, *Cyber Power for the Joint Force Commander*, 14.

¹¹ Angerman, *Cyber Power for the Joint Force Commander*, 3, 5.

¹² Williams, "Ten Propositions Regarding Cyberspace Operations," 11.

not be achieved as long as cyber operations remain segregated from the other warfare mission areas."¹³ Cyberspace as a joint function can better accomplish the mission and give planners the ability to integrate cyberspace with the other six joint functions throughout operational design.

CYBERSPACE AND OPERATIONAL DESIGN

Warfare in this century has adapted to include cyberspace in almost all aspects of joint fighting. Information age fighting has developed a requirement for a JFC to integrate cyberspace to achieve unified action and meet the theater's desired end state.¹⁴ Intelligence efforts are enabled by access to adversary information afforded by cyberspace links. Protection of friendly assets and guaranteed access to cyberspace are crucial to a JFC. JFCs can also utilize cyberspace to enable or support targeting of enemy assets. Theater C2 relies heavily on access and control of cyberspace.

Operations in the 21st-century require access, control, and the ability to shape or influence the cyberspace domain. Making cyberspace a joint function enables the commander to plan and execute joint operations at the timing and tempo of the information age battlefield. The Cyberspace function would support the commander's ability to ensure the protection of friendly access and use of cyberspace while providing for the ability to disrupt, degrade, or destroy adversary cyberspace capabilities. A cyberspace function would reinforce and complement the other six joint functions.

Current doctrine does not capture the reliance on cyberspace to conduct modern war.¹⁵ Cyberspace as a joint function allows commanders and planners to move from

¹³ Rosemary M. Carter, Brent Feick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander," (*JFQ: Joint Force Quarterly* no. 66 (2012 3rd Quarter 2012): 22.

¹⁴ Angerman, *Cyber Power for the Joint Force Commander*, 34.

¹⁵ *Ibid*, 37.

requesting support and coordinating with an externally assigned supporting force, to integrating and synchronizing all assigned assets within the operational design. A cyberspace joint function, integrated and synchronized across the commander's operational design enables the JFC to operate at the speed of an information age.

Joint Publication 5-0, *Joint Operation Planning*, defines operational design as “a process of iterative understanding and problem framing that supports commanders and staffs in their application of operational art with tools and a methodology to conceive of and construct viable approaches to operations and campaigns.”¹⁶ Essentially, operational design “describes the actions the joint force needs to take to reach the end state.” Through the process of creating an operational design, the commander examines the sequences of actions required of the assets assigned to meet the end state, or an examination of ends, ways, and means.¹⁷ Most importantly, the operational design process examines the risk each course of action has, and the risk mitigating factors for the overall operation. Incorporating cyberspace into operational art, as a new joint function, can enable a JFC to utilize cyberspace better to mitigate overall mission risk or to avoid certain options due to specific cyberspace risks.

Like other functions, a JFC will use the cyberspace function across all lines of effort to disrupt, dissuade, or defeat an adversary. Joint Publication 1, notes that “the commander must exercise all the joint functions to effectively operate the force and generate combat power.”¹⁸ A cyberspace joint function is a means to generate combat power at the speed, depth, and breadth on a 21st-century battlefield. Throughout

¹⁶ U.S. Joint Chiefs of Staff, *Joint Operation Planning*, III-1.

¹⁷ Ibid.

¹⁸ U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1, (Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013), I-18.

operational design, an analysis of the enemy's center of gravity and decisive points is performed. This analysis yields certain courses of actions through a series of lines of operations.¹⁹ The adversary situation, friendly capability, and appropriate risk mitigation will help determine if a commander chooses a direct or indirect approach to the operation. Each course of action devises a method for protection of forces to enable the movement and maneuver through the lines of operation. Appropriate fires effect is synchronized to achieve the desired effect on the target. Intelligence and sustainment are planned to support and maintain the operation's effort. A cyberspace function would enhance, support, or enable the other functions to provide a commander the ability to create a 21st-century operational design.

The complexities of cyberspace create uncertainties for planners not familiar with the domain who lack an understanding of how to integrate the capability and synchronize the execution of cyberspace activities. This uncertainty has led to a division of cyberspace planning to geographically separate planners and commanders. To lift the fog of uncertainty surrounding the operational employment of cyberspace, one needs to look to standard operational level planning tools.²⁰ When cyberspace is understood as a function, it can be applied throughout standard processes like the Joint Operational Planning Process, the Joint Targeting Cycle, and Joint Intelligence Preparation of the Operational Environment. All of these planning processes support the commander's operational design and thus are crafted to fit the specifics of the operation.

¹⁹ Refer to U.S. Joint Chiefs of Staff, *Joint Operation Planning*, III-20 – III-32 for a more in-depth look at Center of Gravity, Lines of Effort, Lines of Operations, and Decisive Points.

²⁰ Ibid, 19.

The commander's authorities and allocated assets are matched to achieve the desired end state. Instead of requesting or coordinating for cyberspace effects from outside agencies, a JFC will ensure the strengths and weaknesses of cyberspace are optimized, integrated, and synchronized to meet strategic and operational objectives. Using cyberspace integrated with intelligence, fires, and protection can cause a fog and friction required to compel an enemy to make mistakes.²¹ Israel demonstrated the advantages of cyberspace in creating fog and friction for an adversary to achieve the desired end state with their 2007 conflict with Syria.

In September of 2007 Israel successfully executed a surprise air attack on a suspected Syrian nuclear weapons site at Al-Kibar. Israel demonstrated how 21st-century warfare has changed with proper integration of cyberspace throughout an operation. Although the actual planning documents and commander's assessment are not released to the public, one can speculate the decisions using U.S. planning doctrine. Israel used an operational approach that met the strategic end state of a neutralized Syrian suspected nuclear weapons site with significant constraints and restraints.²² Israeli planners required an approach utilizing a minimal force structure to provide fires on a suspected nuclear weapons complex. The Israeli force needed to maneuver across a Syrian landscape that was heavily protected by an advanced integrated air defense system.

The Israelis demonstrated in their 1981 attack on a suspected Iraqi nuclear weapons plant that they were adept at executing a successful surprise air attack.

However, in 2007 Syria posed a very different threat than Iraq did in 1981. To adjust to

²¹ E. Lincoln Bonner, III, "Cyber Power in 21st-Century Joint Warfare." *JFQ: Joint Force Quarterly* no. 74 (2014 3rd Quarter 2014), 103.

²² U.S. Joint Chiefs of Staff, *Joint Operation Planning*, defines constraints and restraints as action limitations. Constraints are actions that must occur, while restraints are actions that cannot occur, (IV-5).

the changes, Israel needed to turn to a joint function unavailable in 1981, cyberspace. The mission's operational approach demonstrated that Israeli planners had an understanding of a 21st-century battlefield, and more importantly, how to integrate cyberspace at the operational level. If Israel had failed to understand the importance of synchronizing and integrating cyberspace throughout the mission, they would have developed a more indirect approach by kinetically striking individual Syrian air defense nodes to set the conditions for an air strike on the nuclear weapons complex. The indirect approach would have taken longer than one night to execute and potentially cost Israel a greater loss of life and treasure from the higher risk to forces. Instead, Israel turned to a direct approach with the use of integrated cyberspace.

Israel used the function of cyberspace to plan and execute an operation that met the time and force constraints and restraints. Israel synchronized joint operations across all functions, to include cyberspace. The emphasis was on seamlessly operating cyberspace on offensive and defensive actions to enhance the protection of forces for lower risk maneuver and fires. The Israelis integrated use of cyberspace placed the Syrians "at a disadvantage through the flexible application of movement and fires."²³ Israeli air assets were able to maneuver through Syrian airspace unmolested by the modern Syrian air defense who were handicapped by cyberspace.

Operational planners used the synchronized intelligence and cyberspace functions to support a cyberspace attack on the air defense network. Cyberspace attacks created fog and friction for Syrian defenders required to maintain the element of surprise and protect Israeli air assets. The inclusion of cyberspace resulted in an operational design

²³ U.S. Joint Chiefs of Staff, *Joint Operations*, III-28.

which synchronized across all joint functions to tie tactical actions together and meet the strategic objectives with zero Israeli combat losses. Israel demonstrated, in 2007, how 21st-century warfare has changed with the advent of cyberspace as a joint function. The Russians further demonstrated how cyberspace integrated throughout the commander's operational design changed warfare on a much larger scale in the 2008 war between Georgia and Russia.

RUSSIA-GEORGIA WAR CASE STUDY

Isserson defined the change of 19th-century to 20th-century battlefields as one that required a switch in combat design. 20th-century commanders needed to understand the operational design to move away from linear battles to combined arms operations fought in depth.²⁴ Isserson's analysis led him to conclude that warfare was no longer a series of separate tactical actions to meet a strategic end state, but rather connected tactical actions ordered and employed to meet operational objectives.²⁵ The Soviet Red Army employed Isserson's deep battle technique spectacularly during Operation Bagration in June 1944. Here, the Soviet forces combined fires across land and air domains, and planned sustainment to produce a lightning fast advance which ultimately destroyed 30 German Divisions, essentially eliminating the German Army Group Center while advancing 200 miles into Central Europe.²⁶

The Soviets understood what had changed between linear 19th-century battlefields with the advent of the 20th-century maneuver battlefield. Soviet leaders applied Isserson's requirement for a deep battle operational concept and succeeded in

²⁴ Isserson, *Operational Art*, 22-26.

²⁵ Ibid.

²⁶ Williamson Murray and Allan R. Millett. *A War to Be Won: Fighting the Second World War*. (Cambridge, MA: Harvard University Press, 2000), 448-452.

meeting both operational and larger strategic objectives. Today, Russian leaders again have realized the departure from 20th-century maneuver warfare with the 21st-century battlefield. Russia demonstrated its ability to execute on this century's battlefield in their five-day conflict with Georgian forces in the summer of 2008. Russia's use of synchronized cyberspace throughout the operations is beneficial to understanding cyberspace as a joint function.

Russia revealed how cyberspace could be integrated and synchronized for a multi-domain, multi-day, and multiple axis war. Russia added cyberspace across air, land, and maritime forces to ensure their strategic objectives tied to their operational campaign.²⁷ For some, it may seem easy to dismiss the five-day war as a small violent confrontation by a superior Russian military force against a weaker Georgian state. This view, however, fails to discern that the Russia-Georgia war demonstrated the advent of 21st-century warfare.

Russian actions in 2008 challenged assumptions for cyberspace use, and demonstrated how to employ operational art in the 21st-century. Before Russia's operational use of the new domain, cyberspace was assumed to be a complex and dangerous medium only to be used against specific adversaries and only at the strategic level. After August of 2008, one can now question the validity of some previously held assumptions. The first assumption is that cyberspace is only effective against highly technical and internet dependent societies. In 2008, only seven percent of Georgia used the internet.²⁸ Even with this low percentage for an internet based society, Russia

²⁷ George T Donovan, *Russian Operational Art in the Russo-Georgian War of 2008*, Strategic Research Project, (Carlisle Barracks, PA: U.S. Army War College, 2009), 18.

²⁸ Bonner, *Cyber Power in 21st-Century Joint Warfare* 105.

successfully integrated cyberspace in the operational design against Georgia. Second, is the belief that a cyberspace attack would cause a cataclysmic chain of events. Russia displayed an ability to strike targets surgically via cyberspace specifically designed for Georgian targets.²⁹

As discussed earlier, the change in warfare for 21st-century fighting is the timing and tempo due to the speed of cyberspace. The five-day contest demonstrated Russian appreciation of how the timing and tempo of 21st-century warfare have changed. Just as Isserson noted the change to timing and space with maneuver warfare, modern Russian planners understood how to synchronize and integrate cyberspace to optimize the speed of this century's warfare.

Russia designed a military operation to meet three strategic objectives: establish and maintain Russian control over South Ossetia and Abkhazia against any possible Georgian military action; demonstrate to the Georgian people and the Georgian government their dependence on Russia for their security, and to degrade the Georgian military so it would not pose a threat to South Ossetia and Abkhazia.³⁰ The Russian plan looked to overwhelm the Georgian defenses with a combined air, land, sea, and cyberspace assault. Through the campaign's operational design, Russia carefully analyzed Georgian strengths and weaknesses as well as Russian vulnerabilities.

Prior to maneuvering forces into Georgia, Russian planners needed to minimize a Russian critical vulnerability. Russian military planners learned from their conflict with Chechnya that information could be used against Russian operations if the information

²⁹ Ibid, 106.

³⁰ Donovan, *Russian Operational Art*, 7.

environment was not controlled.³¹ To minimize any vulnerability to information operations, the Russians sought to, “shape, control, and suppress the realm of ideas.”³² To accomplish this objective, Russian planners synchronized intelligence, cyberspace, and fires against Georgian information systems. Kinetic strikes on fiber optic connections were combined with Internet denial of service to cut off Georgia's ability to communicate.

Russian planners utilized an axiom from B.H. Liddell Hart by setting conditions prior to fighting that if a battle were to start, it would end quickly.³³ Russia used cyberspace to mitigate a critical vulnerability, while simultaneously attacking a critical strength of Georgia – the ability to command and control forces and communicate with their populace. Russian operational planners synchronized cyberspace activities to create fog and friction, which inhibited Georgia from seizing the initiative or appropriately reacting to the Russian ground offensive. By limiting the Georgian information process, Russia gained the initiative and set a tempo that Georgian forces could not counter. Once Russian forces began to move into Georgia, the initial attacks on the communications infrastructure impeded Georgians from organizing a defense or suitable counter-force.³⁴ In this way, cyberspace was simultaneously executing offensive and defensive operations to synchronize with Russian protection, fires, and movement and maneuver functions. Synchronized naval, air, and land forces maneuvered into South Ossetia, Abkhazia, and established a naval blockade in the Black Sea. Georgia’s military was equipped with

³¹ Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War,” (*Security Dialogue* 43, no. 1 (March 2012)); 8.

³² *Ibid.*, 17.

³³ B.H. Liddell Hart, *Strategy*, 2d rev. ed., (New York: Meridian, 1991), 321.

³⁴ Bonner, *Cyber Power in 21st-Century Joint Warfare*, 107.

modern maneuver warfare equipment, however, Russian superiority with integrated cyberspace neutered any Georgian military response.

Russian operational design combined cyberspace, intelligence, fires, movement and maneuver, and protection throughout the campaign. After cyberspace had achieved the initial objective of degraded Georgian communication nodes, it progressed along the lines of operation to support the movement and maneuver of forces. For example, before the air assault and land maneuver into Gori, Russia attacked city government and local news networks to reduce Georgia's ability to determine and communicate likely avenues of attack.³⁵ Georgia was faced with a multi-axis attack across all domains and did not have an ability to organize its defense, communicate with the Georgian population, or communicate with the outside world.

Warfare since the days of Napoleon has demonstrated the importance of access to information and ability for commanders to disseminate intelligence and coordination maneuvers faster than the enemy could react.³⁶ Synchronizing cyberspace throughout the operational design caused a level of fog and uncertainty for Georgian planners that prevented them from gaining the initiative, establishing a counterforce, or communicating with their population as to the nature and progression of the war. The lack of communication access separated the Georgian government from their people; while the movement and maneuver of Russian ground forces caused confusion, panic, and froze the Georgians into inactivity. Russia controlled the information environment and forced Georgia to act on inaccurate data and delayed their response by denying communication,

³⁵ David Hollis, "Cyberwar Case Study: Georgia 2008," (*Smallwarsjournal.com*. January 6, 2011, <https://www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>. (accessed September 1, 2016)), 6.

³⁶ Smith, *The Utility of Force*, 98-99.

thus enhancing the synchronization of joint functions such as movement and maneuver, protection, intelligence, and cyberspace across the battlespace. Russian planners integrated cyberspace to link tactical actions to the strategic objectives of demonstrating to Georgian people and Georgian government their dependence on Russia and degrading the Georgian military as not to pose a threat to South Ossetia and Abkhazia.

Georgia had a military trained and equipped for 20th-century fighting and was not prepared for the complexities and speed of 21st-century warfare. Subsequently, five days after Georgia's artillery barrage on Tskhinvali in South Ossetia that initiated the Russian reaction, Georgia agreed to Russia's cease-fire terms. Russia had designed a 21st-century operational plan that integrated and synchronized air, land, sea, and cyberspace capabilities. The operational design linked all tactical actions and achieved the three objectives. Eight years later, Abkhazia and South Ossetia are autonomous regions with Russian military bases and Georgia is not a member of EU or NATO.

The Russians, in the 2008 war against Georgia, adjusted operational art for the tempo demands of this century. Russia demonstrated how operational level integration and synchronization of cyberspace defines the modern battlefield. Specific Russian tactics and actions employed in Georgia will most likely not be duplicated. However, it is essential to learn the operational lessons for how to synchronize cyberspace on the 21st-century battlefield. David Hollis noted that "doctrinal concepts such as center of gravity and effects based targeting; and military principals such as mass, economy of force, C2, surprise, and unity of effort apply equally to military operations in the cyberspace domain as to operations in other domains."³⁷

³⁷ Ibid, 8.

Russia demonstrated that cyberspace at the operational level can integrate, synchronize, and direct joint operations. Russian planners combined and synchronized joint functions, to include cyberspace, throughout the operation's design to accomplish their objectives. The operational design centered on invading forces across South Ossetia and Abkhazia. Cyberspace was integrated with fires, intelligence and maneuver to ensure a successful invasion and establish the tempo of operations. Russia showed that like the other six joint functions, cyberspace operates across all levels of war and all military operations.³⁸ Russia used a relatively small force in a synergistic manner to achieve their strategic goals that would not have been possible without the integration of cyberspace. The 2008 war demonstrated that U.S. planners should understand cyberspace as a joint function for JFCs to utilize in future planning. Cyberspace is already being applied as a joint function as the Israeli and Russian examples indicate.

³⁸ Maren Leed, *Offensive Cyber Capabilities at the Operational Level: The Way Forward*, (Washington, DC: Center for Strategic and International Studies, September 2013), 1.

CHAPTER 4: RECOMMENDATIONS

"The only thing harder than getting a new idea into the military mind is to get an old one out" — Sir B.H. Liddell Hart¹

Isserson looked at the lessons of World War I as a revolutionary change to warfare that required the commander to think about a campaign differently and apply the concept of operational art. Isserson's theory of using combined arms in time and space across the battlefield revolutionized 20th-century maneuver warfare. Warfare in the information age requires a similar analysis of operational art with respect to cyberspace. Modern warfare requires a shift from simply trying to integrate cyberspace operations to a thorough understanding of how cyberspace operations are instrumental to the success on the information age battlefield. This requires the integration of cyberspace capabilities at the operational level.

Cyberspace has emerged as an enabling domain to synchronize and coordinate joint operations on the information age battlefield. Military dependence on cyberspace to gather intelligence, position forces, employ weapons, and for protection make the integration of cyberspace throughout operational planning and execution essential. The time has come to move the conversation past who will control and direct cyberspace and begin to devise a way for how the U.S. will use cyberspace at the operational level.

A cyberspace joint function addresses how a JFC will adjust operational art to meet the timing and tempo demands of the 21st-century. This new seventh function will

¹ B.H. Liddell Hart as quoted in James Charlton, ed., *The Military Quotation Book* (New York: St. Martin's Press, 1990), 65.

give JFCs an ability to plan and execute at the speed crucial to maintaining the initiative on the modern battlefield. The expertise needed to plan cyberspace missions at the operational level can come from the already established Cyber Mission Force. JFCs need to strengthen their planning staffs to include cyberspace employment experts. These cyberspace operational planners would need to reside in both the planning and operations branches of a JFC's staff. The cyberspace experts will be the lynchpin to a multi-domain operational design when combined with the other domain, intelligence, and targeting experts on the planning staff. This diverse operational planning team gives JFCs an ability to synchronize joint operations across the joint functions; to include a cyberspace function. The cyberspace function would ensure the protection of friendly access and use of cyberspace while providing the ability to disrupt, degrade or destroy adversary cyberspace.

Individual Services would retain the responsibility to organize, train, and equip cyberspace forces at the tactical level. Each Service will need to foster an inherent cyberspace capability that supports their respective warfighting expertise. The JFC would then have a diverse list of experts to assist with specific planning operations. To plan and execute properly at the operational level, a JFC must have the proper allocated forces and authorities outlined in the operations and execution orders. Authority to use cyberspace capabilities and the necessary forces required for the mission should be looked at in a similar light as every other capability provided to a JFC. Cyberspace operations are as much a part of 21st-century operations as air operations were a century earlier. The allocated cyberspace force combined with cyberspace planners on a JFC

staff provide an ability to fully integrate an operational design to achieve strategic objectives in modern warfare.

At the strategic level, USCYBERCOM would remain the strategic focal point for U.S. cyberspace operations. USCYBERCOM would set the national military cyberspace strategy and maintain the defense of critical U.S. cyberspace infrastructure. Additionally, USCYBERCOM would be the conduit for national level cyberspace operations to a theater commander. Operational level cyberspace planning and execution would be delegated to the appropriate operational level commander.

The Department of Defense and joint staff should adjust current joint doctrine to reflect how a JFC will plan and execute joint operations in the 21st-century. The addition of cyberspace as a joint function grants a JFC the ability to operate on the modern battlefield. Future U.S. operations must include an integrated and synchronized cyberspace function. This will require that a JFC is apportioned a joint force with appropriate cyberspace forces to execute the assigned mission. JFCs must also be delegated the authority to use offensive and defensive cyberspace capabilities to achieve the desired ends. U.S. operational approaches cannot be handicapped with artificial constraints on the employment of joint forces. Similar to how a JFC balances kinetic fires missions against potential cost to intelligence, JFCs must be trusted to balance the value cyberspace operations against intelligence costs with cyberspace fires and protection benefits. A cyberspace joint function provides the operational commander a catalyst to synchronize and integrate joint operations across depth, breadth, space, and time. Cyberspace integration must avoid the painful integration lesson that befell airpower in the early 20th-century.

CHAPTER 5: CONCLUSION

After World War I, U.S. military theorist thought that airpower would change warfare and be the easy path to strategic victory. The U.S. military spent most of the inter war period advocating for different airpower command and control architectures and oversold the strategic potential of airpower. Air enthusiasts were content with the development of bombers and pursuit aircraft that steadily separated air forces from land forces. U.S. military planners were unable to take advantage of the interwar period to organize, train, and equip a force ready to fight in the maneuver warfare of the industrial age.

Conversely, Soviet and German theorists did not concentrate on specific weapons or the new air domain in their reflection on what changed in warfare after the Great War. To these theorists, the change was about speed, integration, and how an operational level commander can synchronize effects. Their knowledge of how the battlefield changed in depth and breadth, and the foresight to understand the speed of an industrial battlefield helped create the theory of operational art. Operational art became the foundation for most industrial militaries to synchronize tactical actions at the speed of an industrial battle to achieve strategic success.

Today, Russia once again demonstrated an understanding of the change in warfare for the information age. While U.S. cyberspace advocates are trying to understand cyberspace power in terms of a 20th-century battlefield, Russia is already employing 21st-century operational design. Like in the period after World War I, Russian military theorists looked beyond individual weapons systems and domains to see how to employ

on the new battlefield. The Georgian-Russian war showcased the depth, breadth, and speed of an information-age battlefield. Cyberspace utilized as a function enabled the Russians to employ an operational design that was unmatched by the Georgians. Russia successfully employed their understanding for what has changed in warfare to demonstrate how cyberspace changed operational design. The speed of the modern battlefield requires synchronization over coordinate effects. The Georgians suffered through the agony of attempting to coordinate activities while their adversary was operating at the speed of cyberspace.

The lessons of history, as well as the practical demonstration of cyberspace as a joint function demand that the U.S. make essential and timely shifts in doctrine and organization. Operations in and through cyberspace are the foundation for executing at the speed and depth of a modern battlefield. Operational planners must understand how to integrate cyberspace across joint service activities. Proper application of cyberspace integrated throughout an operational design is the new requirement.

U.S. planners must move away from static command and control lines of operation and authority and adjust their thinking about cyberspace employment. While it is understood that cyberspace is not the panacea for modern warfare, it is also not a unique arrow in the military quiver reserved for use by commanders outside of the joint operational environment. The current work to create the Cyber Mission Force needs to adapt to organize, train, and equip cyberspace experts in the services who can be allocated or assigned to a joint force commander. Strategic leaders must approve a JFC's authority to protect, operate, and attack in cyberspace. The requirement to bifurcate cyberspace offense and defense operations must adapt to the realities of modern warfare.

Sir Julian Corbett wrote about the need to act in offense and defense in the global commons simultaneously. His axiom on warfare in the global commons must extend to cyberspace. The inclusion of cyberspace as a joint function in U.S. doctrine will enable operational level leaders to plan and execute in the 21st-century. Military leaders in Israel and Russia have already put integrated cyberspace operations into practice and shown the effect in combat. The U.S. military is at a crossroads in history to recognize the evolution from maneuver warfare to information warfare and the change required at the operational level. It is time to include cyberspace as a joint function and advance U.S. operational art to fight on the modern battlefield.

Bibliography

- Angerman, William S. *Cyber Power for the Joint Force Commander: An Operational Design Framework*. Master's Thesis. Norfolk, VA: Joint Advanced Warfighting School, 2014.
- "An Interview with Michael S. Rogers." *JFQ: Joint Force Quarterly* no. 80 (2016 1st Quarter 2016): 78-85.
- Bailey, Jr., Richard J. "Dilating Pupils: The Pedagogy of Cyber Power and the Encouragement of Strategic Thought." *Air and Space Power Journal Africa & Francophonie*. 7, Issue 3 (Fall 2016): 5-25.
- Bender, Jason M. "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations." *Small Wars Journal* 9, no. 11 (November 2013). <http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner> (accessed August 26, 2016)
- "Beyond the Build." *JFQ: Joint Force Quarterly* no. 80 (2016 1st Quarter 2016): 86-93.
- Bilder, Carl H., Steven Bankes, and Richard Nordin. "The Visionary: MacArthur at Inchon." *Command Concepts: A Theory Derived from the Practice of Command and Control* (Santa Monica, CA: Rand Corporation, 1999): 73-87.
- Birdwell, Bodine M. and Robert Mills. "War Fighting in Cyberspace: Evolving Force Presentation and Command and Control." *Air and Space Power Journal* 25, Issue 1 (Spring 2011): 26-36.
- Bonner III, E. Lincoln. "Cyber Power in 21st-Century Joint Warfare." *JFQ: Joint Force Quarterly* no. 74 (2014 3rd Quarter 2014): 102-109. *Academic Search Premier*, EBSCOhost (accessed September 1, 2016).
- Boufesis, Alexandros F. *The Russia-Georgia War of 2008: Russia's Geostrategic Ascension*. Ann Arbor, MI: Nimble Books LLC, 2015.
- Cardon, Edward C., David P. McHenry, and Christopher Cline. 2016. "The Relevance of Culture." *Military Review* 96, no. 4: 34-39. *Academic Search Premier*, EBSCOhost (accessed September 14, 2016).

- Carter, Rosemary M., Brent Feick, and Roy C. Undersander. "Offensive Cyber for the Joint Force Commander." *JFQ: Joint Force Quarterly* no. 66 (2012 3rd Quarter 2012): 22-27. *Academic Search Premier*, EBSCOhost (accessed September 2, 2016).
- Charlton, James. *The Military Quotation Book*. New York: St. Martin's Press, 1990.
- Clarke, Richard A., and Robert K. Kane. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2010.
- Congressional Research Service. *Cyber Operations in DOD Policy and Plans: Issues for Congress*, R43848. Washington DC: Congressional Research Service, January 5, 2015.
- Corbett, Julian S. *Some Principles of Maritime Strategy*. New York: Dover Publications, 2004.
- Cornell, Svante E., and S. Frederick Starr, eds. *The Guns of August 2008. Russia's War in Georgia*. New York: M.E. Sharpe, 2009.
- D'Agostino, Davi M., and Gregory C. Wilshusen. *DOD Faces Challenges in its Cyber Activities*. Washington, D.C.: U.S. Govt. Accountability Office, 2011.
- Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: U.S. Department of Defense, July 2011.
- Deibert, Ronald J., Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War, *Security Dialogue* 43, no. 1 (March 2012): 3-24.
- Donovan, George T., *Russian Operational Art in the Russo-Georgian War of 2008*. Strategic Research Project. Carlisle Barracks, PA: U.S. Army War College, 2009.
- Douhet, Giulio. *The Command of the Air*. Translated by Dino Ferrari. Washington, DC: Office of the Air Force History, 1983.
- Fink, Kallie D., John D. Jordan, and James E. Wells. "Considerations for Offensive Cyberspace Operations." *Military Review* 92, no. 3 (May 2014): 4-11.
- FitzGerald, Ben and Parker Wright. *Digital Theaters: Decentralizing Cyber Command and Control*. Disruptive Defense Papers. Washington, DC: Center for a New American Security, April, 2014.

Fuller, J. F. C. *The Foundations of the Science of War*. Fort Leavenworth, KS: U.S. Army Command and General Staff College Press; 1993.

Gargan, Jason M. "The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects." *Air and Space Power Journal* 30, Issue 1 (Spring 2016): 86-93.

Garamone, Jim. "U.S. Military's Cyber Capabilities Provide Strength, Challenges, Official Says." *Defense.gov*. June 22, 2016.
<http://www.defense.gov/News/Article/810009/us-militarys-cyber-capabilities-provide-strength-challenges-official-says>. (accessed September 1, 2016).

"Georgia, Russia: The Cyberwarfare Angle," *Stratfor.com*. August 12, 2008.
<https://www.stratfor.com/analysis/georgia-russia-cyberwarfare-angle>. (accessed November 11, 2016).

Guderian, Heinz. *Achtung-Panzer!*. Translated by Christopher Duffy. London: Brockhampton Press, 1999.

Hart, B.H. Liddell. *Strategy*, 2d rev. ed. New York: Meridian, 1991.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Smallwarsjournal.com*. January 6, 2011. <https://www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>. (accessed September 1, 2016).

Imparatov, Edward T. *General MacArthur Speeches and Reports 1908-1964*. Paducah, KY: Turner Publishing Company, 2000.

Isserson, Georgii Samoilovich. *The Evolution of Operational Art*. Translated by Bruce W. Menning. Fort Leavenworth, KS: Combat Studies Institute Press, 2013.

Junio, Timothy J. "How Probable is Cyber War? Bringing IR Theory Back Into the Cyber Conflict Debate." *Journal Of Strategic Studies* 36, no. 1 (February 2013): 125-133.

Kern, Sean C.G. "Expanding Combat Power Through Military Cyber Power Theory." *Joint Forces Quarterly* 79 (4th Quarter 2015): 88-95.

Leed, Maren. *Offensive Cyber Capabilities at the Operational Level: The Way Forward*. Washington, DC: Center for Strategic and International Studies, September 2013.

- Libicki, Martin C. "Cyberwar as a Confidence Game" *Strategic Studies Quarterly*, 5, no.1 (Spring 2011): 132-146.
- Lo, Bobo. 2015. *Russia and the New World Disorder*. Washington, DC: Brookings Institution Press, 2015.
- Lyngaas, Sean. "The Quest for Command and Control in Cyberspace." *Federal Computer Week*. July 06, 2015. <https://fcw.com/Articles/2015/06/15/Feature-cybersecurity.aspx?p=1> (accessed August 26, 2016).
- Mahoney, John R. *Reflections on a Strategic Vision for Computer Network Operations*. Strategic Research Project. Carlisle Barracks, PA: U.S. Army War College, 2010.
- Mitchell, William E., *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military*, 2d ed., Tuscaloosa, AL: University of Alabama Press, 2010.
- Montgomery, James. "Division Cyber Operations." *The Cyber Defense Review* [May, 2016]. <http://www.cyberdefensereview.org/2016/05/16/division-cyber-operations/> [accessed September 21, 2016].
- Murray, Williamson and Allan R. Millett. *A War to Be Won: Fighting the Second World War*. Cambridge, MA: Harvard University Press, 2000.
- Myers, Elizabeth A. *Cyber as a "Team Sport": Operationalizing a Whole-of-Government Approach to Cyberspace Operations*. Master's Thesis. Norfolk, VA: Joint Advanced Warfighting School, 2011.
- Ramsby, Corey M., and Panayotis A. Yannakogeorgos. 2016. "A Reality Check on a Cyber Force." *Strategic Studies Quarterly* 10, no. 2: 116-133. *International Security & Counter Terrorism Reference Center*, EBSCOhost (accessed September 1, 2016).
- Regaldo, Daniel, Nart Villeneuve, and John Scott Railton. "Behind the Syrian Conflict's Digital Front Lines." *FireEye.com*. February 2015. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf> (accessed September 1, 2016).
- Reilly, Jeffrey M. "Multidomain Operations: A Subtle but Significant Transition in Military Thought." *Air and Space Power Journal* 30, Issue 1 (Spring 2016): 61-73.

- Reister, Brett. *Cyberspace: Regional and Global Perspectives*. Strategic Research Project. Carlisle Barracks, PA: U.S. Army War College, 2012.
- Rolfe, Robert M., et al. *19th ICCRTS Cyber Operations Model for Multi-Domain Conflict*. Alexandria, VA: Institute for Defense Analyses, April, 2014.
- Schrader, Karl R. *Applying Lessons Learned from Interwar Airpower (1919-1939) to Joint Warfighting with Cyberpower*. [Norfolk, VA]: National Defense University, Joint Forces Staff College, Joint Advanced Warfighting School, 2014.
- Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review* 91, no. 6 (November 2011): 63-68.
- Shakarian, Paulo, Andrew Ruef, and Jana Shakarian. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Amsterdam, Netherlands: Syngress, 2013.
- Singer, Peter W. "The War of Zeros and Ones." *Popular Science*, September, 2014. 40-46.
- Smith, Rupert. *The Utility of Force: The Art of War in the Modern World*. New York: First Vintage Books, 2008.
- Starbuck, F. Randall. *Air Power in North Africa, 1942-43: An Additional Perspective*. Master's Thesis. Carlisle Barracks, PA: U.S. Army War College, 1992.
- Stavridis, James, and David Weinstein. "Time for a U.S. Cyber Force." *U.S. Naval Institute Proceedings* 140, no. 1 (January 2014): 40-44.
- Sutton, Walter S. *Cyber Operations and the Warfighting Functions*. Strategic Research Project. Carlisle Barracks, PA: U.S. Army War College, 2013.
- Tate, Ryan. "Maximizing Flexibility: Mitigating Institutionalized Risk in the Cyber Mission Force." *The Cyber Defense Review*, June, 2016.
<http://www.cyberdefensereview.org/2016/06/28/maximizing-flexibility/> [accessed September 21, 2016].
- The Department of Defense Cyber Strategy*. Washington, DC: U.S. Department of Defense, April 2015.

U.S. Congress. Senate. Armed Services Committee. *Statement of Admiral Michael S. Rogers, USN, Commander, United States Cyber Command*. 114th Cong., 2nd sess., April 5, 2016.

U.S. Cyber Command. *Beyond the Build, Delivering Outcomes through Cyberspace: The Commander's Vision and Guidance for U.S. Cyber Command*. Fort Meade, MD: Department of Defense, June 3, 2015.

U.S. Department of Defense. *Mission Analysis for Cyber Operations of Department of Defense*. Washington, DC: U.S. Department of Defense, August 2014.

_____. *The National Military Strategy of the United States of America, 2015*. Washington DC: U.S. Department of Defense, June 2015.

_____. *Quadrennial Defense Review*, Washington DC: U.S. Department of Defense, 2014.

U.S. Joint Chiefs of Staff. *Capstone Concept for Joint Operations: Joint Force 2020*. Washington, DC: U.S. Joint Chiefs of Staff, September 10, 2012.

_____. *Cyberspace Operations*, Joint Publication 3-12 (R). Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013.

_____. *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 (As Amended Through February 15, 2016).

_____. *Doctrine for the Armed Forces of the United States*, Joint Publication 1. Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013.

_____. *Joint Operations*, Joint Publication 3-0. Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011.

_____. *Joint Operation Planning*, Joint Publication 5-0. Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011.

_____. *Joint Operating Environment 2035*. Washington, DC: Joint Chiefs of Staff, July 14, 2016.

_____. *Joint Targeting*, Joint Publication 3-60. Washington, DC: Joint Chiefs of Staff, January 31, 2013.

_____. *Joint Task Force Headquarters*, Joint Publication 3-33. Washington, DC: U.S. Joint Chiefs of Staff, July 30, 2012.

Wall, Andru E. "Demystifying the Title 10 –Title 50 Debate: Distinguishing Military Operations, Intelligence Activities and Covert Actions." *Harvard National Security Journal* 3 (2011): 85-142.

Williams, Brett T. "Ten Propositions Regarding Cyberspace Operations." *JFQ: Joint Force Quarterly* no. 61 (2011 2nd Quarter 2011): 10-17. (accessed September 2, 2016).

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Forces Quarterly* 73 (2nd Quarter 2014): 12-19.

Wortzel, Larry M. *The Chinese People's Liberation Army and Information Warfare*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2014.

VITA

Lieutenant Colonel Kenneth J. Voigt, Jr., entered the United States Air Force in 1999 through the Reserve Officer Training Corps at Norwich University. He has served as an Air Battle Manager Weapons Officer in the Control and Reporting Center (CRC), Airborne Warning and Control System (AWACS) and served on HQ Air Staff.

Lieutenant Colonel Voigt has participated in Operations ENDURING FREEDOM, AIR DEFENSE OF THE ARABIAN GULF, IRAQI FREEDOM, SOUTHERN WATCH, and counter drug operations. He is a Senior Air Battle Manager with 459 Combat and 104 Combat Support hours in the AWACS additionally with over 2,000 combat hours employing the CRC. Lieutenant Colonel Voigt was granted a Masters of Human Relations degree from the University of Oklahoma and a Master of Arts in National Security and Strategic Studies degree from the Naval War College.

